FORM-PTO-1390 (Rev. 12-29-99) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 032326-136

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5): Unassigned 09/831634

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR99/02692	4 November 1999	12 November 1998

TITLE OF INVENTION: AUTHENTICATING METHOD BETWEEN A SMART CARD AND A TERMINAL

APPLICANT(S) FOR DO/EO/US: Pascal COOREMAN

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and the PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☐ Other items or information:

JC18 Rec'd PCT/PTO 1 1 MAY 2001

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
Unassigned 09/831634	PCT/FR99/02692	032326-136

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $1,000.00 (960)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $860.00 (970)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $710.00 (958)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) $690.00 (956)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00 (962)		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of **$130.00 (154)** for furnishing the oath or declaration later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(e)).	$ -0-	

Claims	Number Filed	Number Extra	Rate		
Total Claims	13 -20 =	-0-	X$18.00 (966)	$ -0-	
Independent Claims	1 -3 =	-0-	X$80.00 (964)	$ -0-	
Multiple dependent claim(s) (if applicable)			+$270.00 (968)	$ -0-	
TOTAL OF ABOVE CALCULATIONS =				$ 860.00	
Reduction for 1/2 for filing by small entity, if applicable (see below).				$ -0-	-
SUBTOTAL =				$ 860.00	
Processing fee of **$130.00 (156)** for furnishing the English translation later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(f)). +				$ -0-	
TOTAL NATIONAL FEE =				$ -0-	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 (581)** per property +				$ -0-	
TOTAL FEES ENCLOSED =				$ 860.00	
				Amount to be: refunded	$
				charged	$

a. ☐ Small entity status is hereby claimed.

b. ☒ A check in the amount of $ 860.00 to cover the above fees is enclosed.

c. ☐ Please charge my Deposit Account No. 02-4800 in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

d. ☐ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

SIGNATURE

James A. LaBarre
NAME

28,632
REGISTRATION NUMBER

Patent
Attorney's Docket No. 032326-136

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Pascal COOREMAN	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: May 11, 2001	)	
	)	
For: AUTHENTICATING METHOD BETWEEN A SMART CARD AND A TERMINAL	)	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows:

IN THE SPECIFICATION:

Page 1, immediately following the title appearing on lines 1 and 2, insert the following:

--This disclosure is based upon, and claims priority from French Application No. 98/14224, filed on November 12, 1998 and International Application No. PCT/FR99/02692, filed November 4, 1999, which was published on May 25, 2000 in a language other than English, the contents of which are incorporated herein by reference.

Background of the Invention--

Page 2, between lines 7 and 8, insert the following heading:

--**Summary of the Invention** --.

Page 3, between lines 25 and 26, insert the following heading:

--**Brief Description of the Drawings**--.

Page 4, between lines 5 and 6, insert the following heading:

--**Detailed Description**--.

IN THE CLAIMS:

Kindly replace claims 1-13, as follows.

1. (Amended) An authenticating method between a memory chip card having at least one counter and a terminal, comprising the following steps:

(a) inserting the memory chip card into the terminal,

(b) calculating, in the terminal, a secret code CSC_1 according to a cryptographic function F of a number of variables comprising at least a code CSN identifying the memory chip card and the value of said counter,

(c) authenticating the terminal by the card when the calculated secret code CSC_1 is identical to a code CSC_0 recorded in a memory of the card at the end of a previous authentication operation,

(d) carrying out a desired transaction and modifying the value of said counter,

(e) calculating, in the terminal, a new secret code CSC_2 according to the cryptographic function F of the code CSN identifying the memory chip card and the new value of said counter,

(f) updating the memory chip card for the next transaction by recording, in said memory, the new secret code CSC_2 calculated by the operation (e).

2. (Amended) A method according to Claim 1, further including the following steps between the steps (c) and (d):

(x) calculating, in the terminal, an authentication certificate CA_1 according to a cryptographic function G of a number of variables comprising at least the code CSN identifying the memory chip card and the value of the counter,

(y) authenticating the card by the terminal when the calculated authentication certificate CA_1 is identical to a certificate CA_0 calculated and recorded at the end of the previous transaction,

and wherein step (e) is supplemented by the step of

(e′) calculating, in the terminal, a new authentication certificate CA_2 according to the cryptographic function G of the code CSN identifying the memory chip card and the new value of said counter,

- and wherein step (f) is supplemented by the step of

(f′) updating the memory chip card for the next transaction by recording, in the memory, the new authentication certificate CA_2 calculated according to the step (e′).

3. (Amended) A method according to Claim 2 wherein step (b) comprises the following steps:

- first calculating, in the terminal, a session key K_{s1} according to a cryptographic function F_{ks} of a number of variables comprising at least a parent key K_m known by the terminal, the code CSN identifying the memory chip card and the value of said counter,

- next calculating, in the terminal, the secret code CSC_1 according to the cryptographic function F of the session key K_{s1},

and wherein step (e) comprises:

- first calculating, in the terminal, a new session key K_{s2} according to the cryptographic function F_{ks} with the new value of said counter,

- next calculating, in the terminal, the new secret code CSC_2 according to the cryptographic function F of the new session key K_{s2}.

4. (Amended) A method according to Claim 3 wherein step (e') includes the step of calculating the new authentication certificate CA_2 according to the cryptographic function G of the new session key K_{s2}.

5. (Amended) A method according to claim 1 wherein the memory chip card comprises two counters, one counting the authentications and the other counting payment transactions, and wherein the variables of the cryptographic functions comprise the values of said counters.

6. (Amended) A method according to claim 1 wherein the cryptographic functions are one-way functions.

7. (Amended) A method according to Claim 6, wherein the cryptographic functions are "hashing" functions.

8. (Amended) A method according to claim 3, wherein step (b) comprises the following steps:

(b_1) reading the serial number CSN of the card,

(b_2) reading the content of the counter, and

(b_3) calculating the session key according to a cryptographic function F_{ks} such that:

$Ks_1 = F_{ks} (K_m, CSN, CTC_1)$.

9. (Amended) A method according to claim 1, wherein step (c) comprises the following steps:

(c_1) transmitting the secret code CSC_1 to the card,

(c_2) comparing, in the card, this secret code CSC_1 with a secret code CSC_0 recorded in the card at the end of the previous transaction with the card, and

(c_3) authorizing the remainder of the operations if the comparison indicates the identity $CSC_0 = CSC_1$ or refusing same if CSC_0 is not equal to CSC_1.

10. (Amended) A method according to claim 2, wherein step (y) comprises the following steps:

(y_1) reading the content CA_0 of a designated area of the memory of the card CM,

(y_2) transmitting, to the terminal, the content CA_0 of said area which corresponds to an Authentication Certificate CA_0 calculated at the end of the previous transaction,

(y_3) comparing, in the terminal, the calculated Authentication Certificate CA_1 with the certificate CA_0, and

(y_4) authorizing the remainder of the operations if the comparison indicates the identify $CA_1 = CA_0$.

11. (Amended) A method according to claim 1, wherein step (d) comprises the following steps:

(d_1) reading, from an area of the memory, the value BAL_0 of a balance resulting from the previous transaction and a corresponding certificate $CBAL_0$, and

(d_2) verifying that the certificate $CBAL_0$ correctly corresponds to the result of the cryptographic function such that:

$CBAL_0 = H (K_t, BAL_0, CSN, CTC_1)$,

- K_t being a transaction key,

(d_3) incrementing the transaction counter to the value $(CTC_1 + 1) = CTC_2$.

(d_4) recording the new balance BAL_1 in said area,

(d_5) calculating a Certificate $CBAL_1$ for the new balance BAL_1 such that:

$CBAL_1 = H (K_t, BAL_1, CSN, CTC_2)$, and

(d_6) recording $CBAL_1$ in said area.

12. (Amended) A method according to claim 1 wherein step (a) also comprises a step of entering a personal code of the user.

13. (Amended) A method according to claim 3, wherein in step (b), one of the variables used for calculating the session key Ks_1 is a personal code PIN of the user.

Add the following new claims:

14. (New) A method according to Claim 1 wherein step (b) comprises the following steps:

- first calculating, in the terminal, a session key K_{s1} according to a cryptographic function F_{ks} of a number of variables comprising at least a parent key K_m known by the terminal, the code CSN identifying the memory chip card and the value of said counter,

- next calculating, in the terminal, the secret code CSC_1 according to the cryptographic function F of the session key K_{s1},

and wherein step (e) comprises:

- first calculating, in the terminal, a new session key K_{s2} according to the cryptographic function F_{ks} with the new value of said counter,

- next calculating, in the terminal, the new secret code CSC_2 according to the cryptographic function F of the new session key K_{s2}.

15. (New) A method according to claim 14, wherein step (b) comprises the following steps:

(b_1) reading the serial number CSN of the card,

(b_2) reading the content of the counter, and

(b_3) calculating the session key according to a cryptographic function F_{ks} such that:

$$Ks_1 = F_{ks} (K_m, CSN, CTC_1).$$

REMARKS

Entry of the foregoing amendment is respectfully requested. This amendment is intended to place the claims in a more conventional format and eliminate the multiple dependency of the claims.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: [signature]
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: May 11, 2001

Attachment to Preliminary Amendment dated May 11, 2001

Marked-up Claims 1-13

1. (Amended) An authenticating method between a memory chip card [(CM)] having at least one counter [(CE, CT)] and a terminal [(TE), characterised in that it comprises], comprising the following steps [consisting of]:

(a) inserting the memory chip card [(CM)] into the terminal [(TE)],

(b) calculating, in the terminal, a secret code CSC_1 according to a cryptographic function F of a number of variables comprising at least a code CSN identifying the memory chip card and the value [(CTE_1, CTC_1)] of said counter [(CE, CT)],

(c) authenticating the terminal by the card when the calculated secret code CSC_1 is identical to a code CSC_0 recorded in [the] a memory of the card at the end of [the] a previous authentication [according to the] operation [(f) below],

(d) carrying out [the planned] a desired transaction and modifying the value [(CTE_2, CTC_2)] of said counter [(CE, CT)],

(e) calculating, in the terminal [(TE)], a new secret code CSC_2 according to the cryptographic function F of the code CSN identifying the memory chip card [(CM)] and the new value [(CTE_2, CTC_2)] of said counter [(CE, CT)],

(f) updating the memory chip card [(CM)] for the next transaction by recording, in [the] said memory [(M)], the new secret code CSC_2 calculated by the operation (e).

2. (Amended) A method according to Claim 1, [characterised:

Attachment to Preliminary Amendment dated May 11, 2001

Marked-up Claims 1-13

- in that it comprises] further including the following [supplementary] steps between the steps (c) and (d) [consisting of]:

(x) calculating, in the terminal [(TE)], an authentication certificate CA_1 according to a cryptographic function G of a number of variables comprising at least the code CSN identifying the memory chip card and the value [(CTE_1, CTC_1)] of the counter [(CE, CT)],

(y) authenticating the card [(CM)] by the terminal [(TE)] when the calculated authentication certificate CA_1 is identical to a certificate CA_0 calculated and recorded at the end of the previous transaction [according to the steps (e′) and (f′) below:

- in that the], and wherein step (e) is supplemented by the [following] step [consisting] of[:]

(e′) calculating, in the terminal [(TE)], a new authentication certificate CA_2 according to the cryptographic function G of the code CSN identifying the memory chip card and the new value [(CTE_2, CTC_2)] of said counter [(CE, CT)],

- and [in that the] wherein step (f) is supplemented by the [following] step [consisting] of[:]

(f′) updating the memory chip card [(CM)] for the next transaction by recording, in the memory [(M)], the new authentication certificate CA_2 calculated according to the step (e′).

3. (Amended) A method according to Claim [1, characterised:

Attachment to Preliminary Amendment dated May 11, 2001

Marked-up Claims 1-13

- in that the step (b) consists of:] 2 wherein step (b) comprises the following steps:

- first calculating, in the terminal [(TE)], a session key K_{s1} according to a cryptographic function F_{ks} of a number of variables comprising at least a parent key K_m known by the terminal [(TE)], the code CSN identifying the memory chip card [(CM)] and the value [(CTE_1, CTC_1)] of said counter [(CE, CT)],

- next calculating, in the terminal [(TE)], the secret code CSC_1 according to the cryptographic function F of the session key K_{s1},

[- in that the step (e) consists of:] and wherein step (e) comprises:

- first calculating, in the terminal [(TE)], a new session key K_{s2} according to the cryptographic function F_{ks} with the new value [(CTE_2, CTC_2)] of said counter [(CE, CT)],

- next calculating, in the terminal [(TE)], the new secret code CSC_2 according to the cryptographic function F of the new session key K_{s2}.

4. (Amended) A method according to Claim [2 and 3, characterised in that:

- the step (e') consists] 3 wherein step (e') includes the step of calculating the new authentication certificate CA_2 according to the cryptographic function G of the new session key K_{s2}.

5. (Amended) A method according to [any one of the previous Claims 1 to 4, in its application to a] claim 1 wherein the memory chip card [(CM) comprising] comprises

Attachment to Preliminary Amendment dated May 11, 2001

Marked-up Claims 1-13

two counters, one [(CE)] counting the authentications and the other [(CT)] counting [the] payment transactions, [characterised in that] and wherein the variables of the cryptographic functions [F, G and F_{ks}] comprise the values [(CTE_1, CTE_2, CTC_1, CTC_2)] of said counters.

6. (Amended) A method according to [one of the previous claims, characterised in that] claim 1 wherein the cryptographic functions [F, G and F_{ks}] are one-way functions.

7. (Amended) A method according to Claim 6, [characterised in that] wherein the cryptographic functions [F, G and F_{ks}] are "hashing" functions.

8. (Amended) A method according to [one of the previous Claims 3 to 7, characterised in that the] claim 3, wherein step (b) comprises the following steps [consisting of]:

(b_1) reading the serial number CSN of the card [(CM)],

(b_2) reading the content [(CTE_1 and/or CTC_1)] of the counter, and

(b_3) calculating the session key according to a cryptographic function F_{ks} such that:

$$Ks_1 = F_{ks} (K_m, CSN, CTC_1).$$

Attachment to Preliminary Amendment dated May 11, 2001

Marked-up Claims 1-13

9. (Amended) A method according to [one of Claims 1 to 8, characterised in that the] claim 1, wherein step (c) comprises the following steps [consisting of]:

(c_1) transmitting the secret code CSC_1 to the card [CM],

(c_2) comparing, in the card, this secret code CSC_1 with a secret code CSC_0 recorded in the card [CM] at the end of the previous transaction with the card, and

(c_3) authorizing the remainder of the operations if the comparison indicates the identity $CSC_0 = CSC_1$ or refusing same [in the contrary case] if CSC_0 is not equal to CSC_1.

10. (Amended) A method according to [one of Claims 2 to 9, characterised in that the] claim 2, wherein step (y) comprises the following steps [consisting of]:

(y_1) reading the content CA_0 of [the area ZCA] a designated area of the memory of the card CM,

(y_2) transmitting, to the terminal [(TE)], the content CA_0 of [this area ZCA] said area which corresponds to an Authentication Certificate CA_0 calculated at the end of the previous transaction,

(y_3) comparing, in the terminal [TE], the calculated Authentication Certificate CA_1 with the certificate CA_0, and

(y_4) authorizing the remainder of the operations if the comparison indicates the identify $CA_1 = CA_0$.

Attachment to Preliminary Amendment dated May 11, 2001

Marked-up Claims 1-13

11. (Amended) A method according to [one of Claims 1 to 10, characterised in that the] claim 1, wherein step (d) comprises[, in the case of modification of the balance BAL_0,] the following steps [consisting of]:

(d_1) reading, from an area [ZBAL] of the memory [(M)], the value BAL_0 of [the] a balance resulting from the previous transaction and [the] a corresponding certificate $CBAL_0$, and

(d_2) verifying that the certificate $CBAL_0$ correctly corresponds to the result of the cryptographic function such that:

$CBAL_0 = H (K_t, BAL_0, CSN, CTC_1)$,

- K_t being a transaction key,

(d_3) incrementing the transaction counter to the value $(CTC_1 + 1) = CTC_2$.

(d_4) recording the new balance BAL_1 in [the] said area [ZBAL],

(d_5) calculating a Certificate $CBAL_1$ for the new balance BAL_1 such that:

$CBAL_1 = H (K_t, BAL_1, CSN, CTC_2)$, and

(d_6) recording $CBAL_1$ in [the] said area [ZBAL].

12. (Amended) A method according to [one of the previous Claims 1 to 11, characterised in that:

- the] claim 1 wherein step (a) also comprises a step of entering [the] a personal code [PIN] of the user.

Attachment to Preliminary Amendment dated May 11, 2001

Marked-up Claims 1-13

13. (Amended) A method according to [one of the previous Claims 3 to 12, characterised in that:

- in the] claim 3, wherein in step (b), one of the variables used for calculating the session key Ks_1 is [the] a personal code PIN of the user.

AUTHENTICATING METHOD BETWEEN A SMART CARD AND A TERMINAL

The invention concerns memory chip cards and the terminals to which they are capable of being connected from time to time and, more particularly, a method which enables the memory chip card and the terminal to authenticate one another.

Memory chip cards, on account of their not having a microprocessor, cannot use an authentication algorithm which involves calculations. However, certain memory chip cards use an algorithm in hard-wired form which allows the so-called "active" authentication of the card by the terminal but not the reverse authentication of the terminal by the card. Owing to their low cost, memory chip cards are used a great deal in many applications such as loyalty cards, access control, charge card payments, etc. However, owing to the lack of authentication, their security in use is vulnerable so that microprocessor cards are sometimes preferred to them for certain applications. But these microprocessor cards have a distinctly higher cost, which becomes increasingly higher as the authentication algorithm becomes more developed, which leads to them being ruled out for inexpensive applications. Also, the aim of the present invention is to obtain security in use of memory chip cards.

This aim is achieved by using an authentication method in which all the algorithmic calculations are

performed by the terminal to which the memory chip card is connected.

Furthermore, the operations relating to authentication are performed before the start of a transaction proper and after the end of this transaction with a view to the authentication at the start of the following transaction.

The invention therefore concerns an authenticating method between a memory chip card having at least one counter and a terminal, characterised in that it comprises the following steps consisting of:

(a) inserting the memory chip card into the terminal,

(b) calculating, in the terminal, a secret code CSC_1 according to a cryptographic function F of a number of variables comprising at least a code CSN identifying the memory chip card and the value of said counter,

(c) authenticating the terminal by the card when the calculated secret code CSC_1 is identical to a code CSC_0 recorded in the memory at the end of the previous authentication according to the operation (f) below,

(d) carrying out the planned transaction and modifying the value of said counter,

(e) calculating, in the terminal, a new secret code CSC_2 according to the cryptographic function F of the code CSN identifying the memory chip card and the new value of said counter,

(f) updating the memory chip card for the next transaction by recording, in the memory, the new secret code CSC_2 calculated by the operation (e).

In order to obtain authentication of the card by the terminal, the method comprises the following supplementary steps between the steps (c) and (d) consisting of:

(x) calculating, in the terminal, an authentication certificate CA_1 according to a cryptographic function G of a number of variables comprising at least the code CSN identifying the memory chip card and the value of said counter,

(y) authenticating the card by the terminal when the calculated authentication certificate CA_1 is identical to a certificate CA_0 calculated and recorded in the card at the end of the previous transaction according to the steps (e') and (f') below:

- in that the step (e) is supplemented by the following step consisting of:

(e') calculating, in the terminal, a new authentication certificate CA_2 according to the cryptographic function G,

- and in that the step (f) is supplemented by the following step consisting of:

(f') updating the memory chip card for the next transaction by recording, in the memory, the new authentication certificate CA_2 calculated according to the step (e').

Other characteristics and advantages of the present invention will emerge from a reading of the following description of a particular embodiment, said description being given with reference to the accompanying drawing in which:

- Figure 1 is a simplified diagram of a memory chip card, and

- Figure 2 is a chart showing the operations performed between the terminal and the memory chip card during a transaction.

The method of the invention applies (Figure 1) to a memory chip card CM which of course comprises a memory M but also a so-called transaction counter CT which counts the transactions performed between the card CM and a terminal TE to which the card is connected by insertion.

The memory chip card CM can also comprise a second so-called authentication counter CE which counts the authentication requests, these authentication requests possibly occurring at any time during a transaction and independently thereof.

These two counters CE and CT can form part of the memory M according to known devices.

In addition, the memory M of the card comprises a first area with unprotected read access in which there is recorded, for example the serial number CSN of the card in a part ZCSN, and a second area with protected access for the rest of the memory, this second area having parts which are allocated to the recording of particular values such as an Authentication Certificate CA in the part ZCA and a balance BAL and its authentication certificate CBAL in the part ZBAL.

A third area ZCSC is reserved for the recording of a secret code CSC and its access for recording is subject to presentation of the secret code CSC.

The memory M is addressed by an addressing circuit ADR and the two-way transmission of signals between the terminal TE and the card CM takes place by means of an interface circuit INT.

Furthermore, the card comprises a comparator CP which compares the code CSC read from the part ZCSC with a code supplied by the terminal TE, the result of the comparison allowing or not allowing the addressing of the protected area of the memory M.

The method according to the invention will be described within the context of a mutual authentication between the card and the terminal using the transaction counter CT alone and so-called one-way cryptographic functions but the method of the invention can also apply to authentication of the terminal by the card alone, and to simultaneous use of the two counters CE and CT and cryptographic functions other than one-way ones. The various operations, notably cryptographic operations, can be carried out either in the terminal TE, or in a security module, or even in a remote device.

Preferably, the mutual authentication method according to the invention comprises the following steps consisting of:

(m) inserting the card CM into the terminal TE, this step possibly including the presentation of a personal code PIN of the card user,

(n) calculating, in the terminal TE, a session key Ks_1 by:

(n_1) reading the serial number CSN of the card CM,

(n_2) reading the content CTC_1 of the transaction counter CT of the card CM, and

(n_3) calculating a session key Ks_1 according to a one-way cryptographic function F_{ks} such that:

$Ks_1 = F_{ks}(K_m, CSN, CTC_1)$

- K_m being a parent key recorded in the terminal TE,

- F_{ks} being for example a function of the hashing type,

(o) calculating, in the terminal TE, a secret code CSC_1 of the card using a cryptographic function F such that:

$CSC_1 = F(Ks_1)$,

(p) authenticating the terminal TE by the card CM by:

(p_1) transmitting the secret code CSC_1 to the card CM,

(p_2) comparing, in the comparator CP, this secret code CSC_1 with a secret code CSC_0 recorded in the card CM at the end of the previous transaction with the card, and

(p_3) authorizing the remainder of the operations if the comparison indicates the identity $CSC_0 = CSC_1$ or refusing same in the contrary case;

(q) calculating, in the terminal TE, an Authentication Certificate CA_1 such that:

$CA_1 = G(Ks_1)$

- G being a cryptographic function, and

(r) authenticating the card CM by the terminal TE by:

(r_1) reading the content CA_0 of the area ZCA of the memory of the card CM,

(r_2) transmitting, to the terminal TE, the content CA_0 of this protected area ZCA which corresponds to an Authentication Certificate CA_0 calculated at the end of the previous transaction,

(r_3) comparing, in the terminal TE, the calculated Authentication Certificate CA_1 with the certificate CA_0, and

(r_4) authorizing the remainder of the operations if the comparison indicates the identity $CA_1 = CA_0$;

(s) carrying out the transaction, this transaction possibly consisting for example of updating a memory area ZBAL indicating the state of the credit or balance BAL remaining in the card CM by:

(s_1) reading, from the area ZBAL, the value BAL_0 of the balance resulting from the previous transaction and the corresponding certificate $CBAL_0$,

(s_2) verifying that the certificate $CBAL_0$ correctly corresponds to the result of the cryptographic function such that:

$CBAL_0 = H(K_t, BAL_0, CSN, CTC_1)$,

- K_t being a transaction key,

(s_3) incrementing the transaction counter to the value $(CTC_1 + 1) = CTC_2$

(s_4) recording the new balance BAL_1 in the area ZBAL,

(s_5) calculating a Certificate $CBAL_1$ for the new balance BAL_1 such that:

$CBAL_1 = H(K_t, BAL_1, CSN, CTC_2)$, and

(s_6) recording $CBAL_1$ in the area ZBAL;

(t) updating the card CM for the next transaction with a new secret code CSC_2 and a new certificate CA_2, by

(t_1) calculating in the terminal TE:

- the future session key Ks_2 such that:

$Ks_2 = F(K_m, CSN, CTC_2)$

- the future secret code CSC_2 such that:

$CSC_2 = F(Ks_2)$,

- the future authentication certificate CA_2 such that:

$CA_2 = G(Ks_2)$,

(t_2) recording the secret code CSC_2 in the memory M of the card CM in the protected area and the authentication certificate CA_2 in the protected area ZCA.

The invention has been described with a particular embodiment in which the transaction is an operation on the balance value of the card; however, the invention applies to any other transaction according to the applications provided for the card under consideration.

In this particular example, the transaction ends with an incrementing of the transaction counter CT to a value CTC_2 which is usually equal to $(CTC_1 + 1)$. However, this value of CTC_2 can be different from $(CTC_1 + 1)$ and be equal, for example, to $(CTC_1 + 3)$.

This transaction counter must be incremented or decremented at each transaction even if the operation leads to the balance not being changed; in this case, it is necessary to perform the transaction by re-recording the unchanged balance but the certificate $CBAL_1$ will be different since the transaction counter will have been incremented. The same will apply for the new secret code CSC_2 and the certificate CA_2.

The variables of the functions F, G and F_{ks} which have been adopted in the example are the parent key, the serial number CSN and the value CTC of the transaction counter. However, additional variables can be used such as the personal code PIN of the card user, this code being entered into the terminal after insertion of the card.

The invention has been described within the context of a card/terminal mutual authentication but it applies more generally first to an authentication of the terminal by the card, this first authentication possibly being followed or not followed by an authentication of the card by the terminal, the set of these two authentications making a mutual authentication.

The example described uses cryptographic functions F, G and F_{ks} using variables such as a parent key K_m, a session key K_s and a transaction key K_t, but such keys are not necessary for implementing the invention.

The value of the authentication counter CE is preferably used for calculating the secret code CSN

while the value of the transaction counter CT is preferably used for calculating the authentication certificate CA.

CLAIMS

1. An authenticating method between a memory chip card (CM) having at least one counter (CE, CT) and a terminal (TE), characterised in that it comprises the following steps consisting of:

(a) inserting the memory chip card (CM) into the terminal (TE),

(b) calculating, in the terminal, a secret code CSC_1 according to a cryptographic function F of a number of variables comprising at least a code CSN identifying the memory chip card and the value (CTE_1, CTC_1) of said counter (CE, CT),

(c) authenticating the terminal by the card when the calculated secret code CSC_1 is identical to a code CSC_0 recorded in the memory at the end of the previous authentication according to the operation (f) below,

(d) carrying out the planned transaction and modifying the value (CTE_2, CTC_2) of said counter (CE, CT),

(e) calculating, in the terminal (TE), a new secret code CSC_2 according to the cryptographic function F of the code CSN identifying the memory chip card (CM) and the new value (CTE_2, CTC_2) of said counter (CE, CT),

(f) updating the memory chip card (CM) for the next transaction by recording, in the memory (M), the new secret code CSC_2 calculated by the operation (e).

2. A method according to Claim 1, characterised:

- in that it comprises the following supplementary steps between the steps (c) and (d) consisting of:

(x) calculating, in the terminal (TE), an authentication certificate CA_1 according to a cryptographic function G of a number of variables comprising at least the code CSN identifying the memory chip card and the value (CTE_1, CTC_1) of the counter (CE, CT),

(y) authenticating the card (CM) by the terminal (TE) when the calculated authentication certificate CA_1 is identical to a certificate CA_0 calculated and recorded at the end of the previous transaction according to the steps (e') and (f') below:

- in that the step (e) is supplemented by the following step consisting of:

(e') calculating, in the terminal (TE), a new authentication certificate CA_2 according to the cryptographic function G of the code CSN identifying the memory chip card and the new value (CTE_2, CTC_2) of said counter (CE, CT),

- and in that the step (f) is supplemented by the following step consisting of:

(f') updating the memory chip card (CM) for the next transaction by recording, in the memory (M), the new authentication certificate CA_2 calculated according to the step (e').

3. A method according to Claim 1, characterised:

- in that the step (b) consists of:

- first calculating, in the terminal (TE), a session key K_{s1} according to a cryptographic function F_{ks} of a number of variables comprising at least a parent key K_m known by the terminal (TE), the code CSN identifying the memory chip card (CM) and the value (CTE_1, CTC_1) of said counter (CE, CT),

- next calculating, in the terminal (TE), the secret code CSC_1 according to the cryptographic function F of the session key K_{s1},

- in that the step (e) consists of:

- first calculating, in the terminal (TE), a new session key K_{s2} according to the cryptographic function F_{ks} with the new value (CTE_2, CTC_2) of said counter (CE, CT),

- next calculating, in the terminal (TE), the new secret code CSC_2 according to the cryptographic function F of the new session key K_{s2}.

4. A method according to Claim 2 and 3, characterised in that:

- the step (e') consists of calculating the new authentication certificate CA_2 according to the cryptographic function G of the new session key K_{s2}.

5. A method according to any one of the previous Claims 1 to 4, in its application to a memory chip card (CM) comprising two counters, one (CE) counting the authentications and the other (CT) counting the payment transactions, characterised in that the variables of the cryptographic functions F, G and F_{ks} comprise the values (CTE_1, CTE_2, CTC_1, CTC_2) of said counters.

6. A method according to one of the previous claims, characterised in that the cryptographic functions F, G and F_{ks} are one-way functions.

7. A method according to Claim 6, characterised in that the cryptographic functions F, G and F_{ks} are "hashing" functions.

8. A method according to one of the previous Claims 3 to 7, characterised in that the step (b) comprises the following steps consisting of:

(b_1) reading the serial number CSN of the card (CM),

(b_2) reading the content (CTE_1 and/or CTC_1) of the counter, and

(b_3) calculating the session key according to a cryptographic function F_{ks} such that:

$Ks_1 = F_{ks} (K_m, CSN, CTC_1)$.

9. A method according to one of Claims 1 to 8, characterised in that the step (c) comprises the following steps consisting of:

(c_1) transmitting the secret code CSC_1 to the card CM,

(c_2) comparing, in the card, this secret code CSC_1 with a secret code CSC_0 recorded in the card CM at the end of the previous transaction with the card, and

(c_3) authorizing the remainder of the operations if the comparison indicates the identity $CSC_0 = CSC_1$ or refusing same in the contrary case.

10. A method according to one of Claims 2 to 9, characterised in that the step (y) comprises the following steps consisting of:

(y_1) reading the content CA_0 of the area ZCA of the memory of the card CM,

(y_2) transmitting, to the terminal (TE), the content CA_0 of this area ZCA which corresponds to an Authentication Certificate CA_0 calculated at the end of the previous transaction,

(y_3) comparing, in the terminal TE, the calculated Authentication Certificate CA_1 with the certificate CA_0, and

(y_4) authorizing the remainder of the operations if the comparison indicates the identity $CA_1 = CA_0$.

11. A method according to one of Claims 1 to 10, characterised in that the step (d) comprises, in the case of modification of the balance BAL_0, the following steps consisting of:

(d_1) reading, from an area ZBAL of the memory (M), the value BAL_0 of the balance resulting from the previous transaction and the corresponding certificate $CBAL_0$, and

(d_2) verifying that the certificate $CBAL_0$ correctly corresponds to the result of the cryptographic function such that:

$CBAL_0 = H(K_t, BAL_0, CSN, CTC_1)$,

- K_t being a transaction key,

(d_3) incrementing the transaction counter to the value $(CTC_1 + 1) = CTC_2$

(d_4) recording the new balance BAL_1 in the area ZBAL,

(d_5) calculating a Certificate $CBAL_1$ for the new balance BAL_1 such that:

$CBAL_1 = H(K_t, BAL_1, CSN, CTC_2)$, and

(d_6) recording $CBAL_1$ in the area ZBAL.

12. A method according to one of the previous Claims 1 to 11, characterised in that:

- the step (a) also comprises a step of entering the personal code PIN of the user.

13. A method according to one of the previous Claims 3 to 12, characterised in that:

- in the step (b), one of the variables used for calculating the session Ks_1 is the personal code PIN of the user.

09/831634

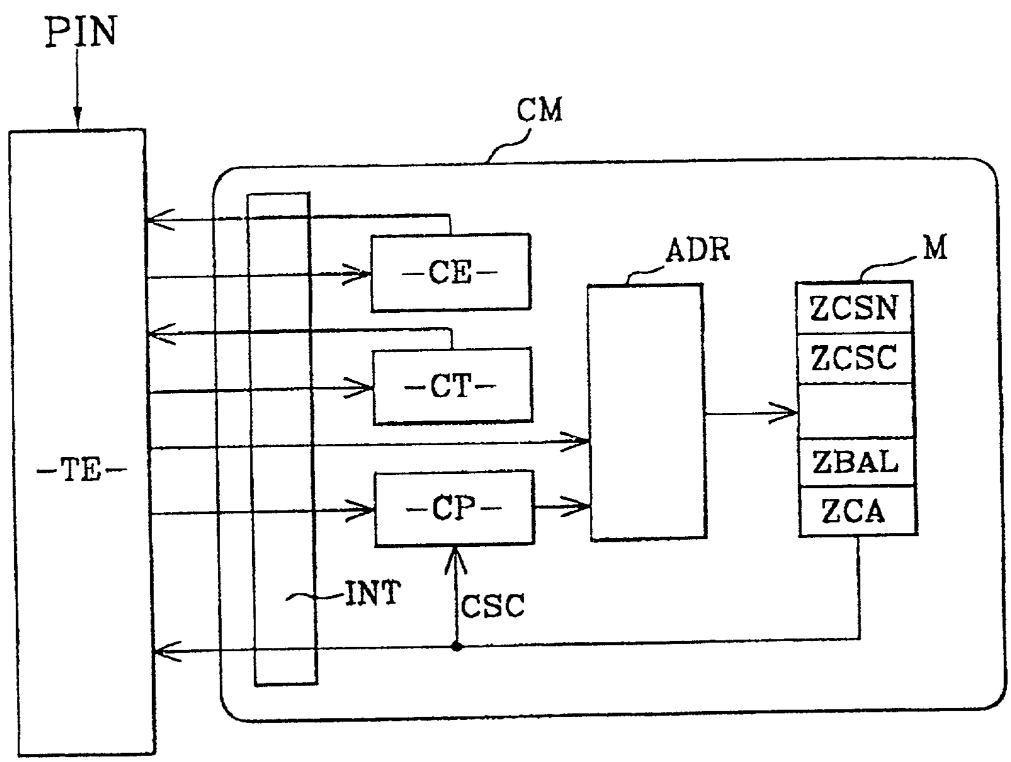

FIG.1

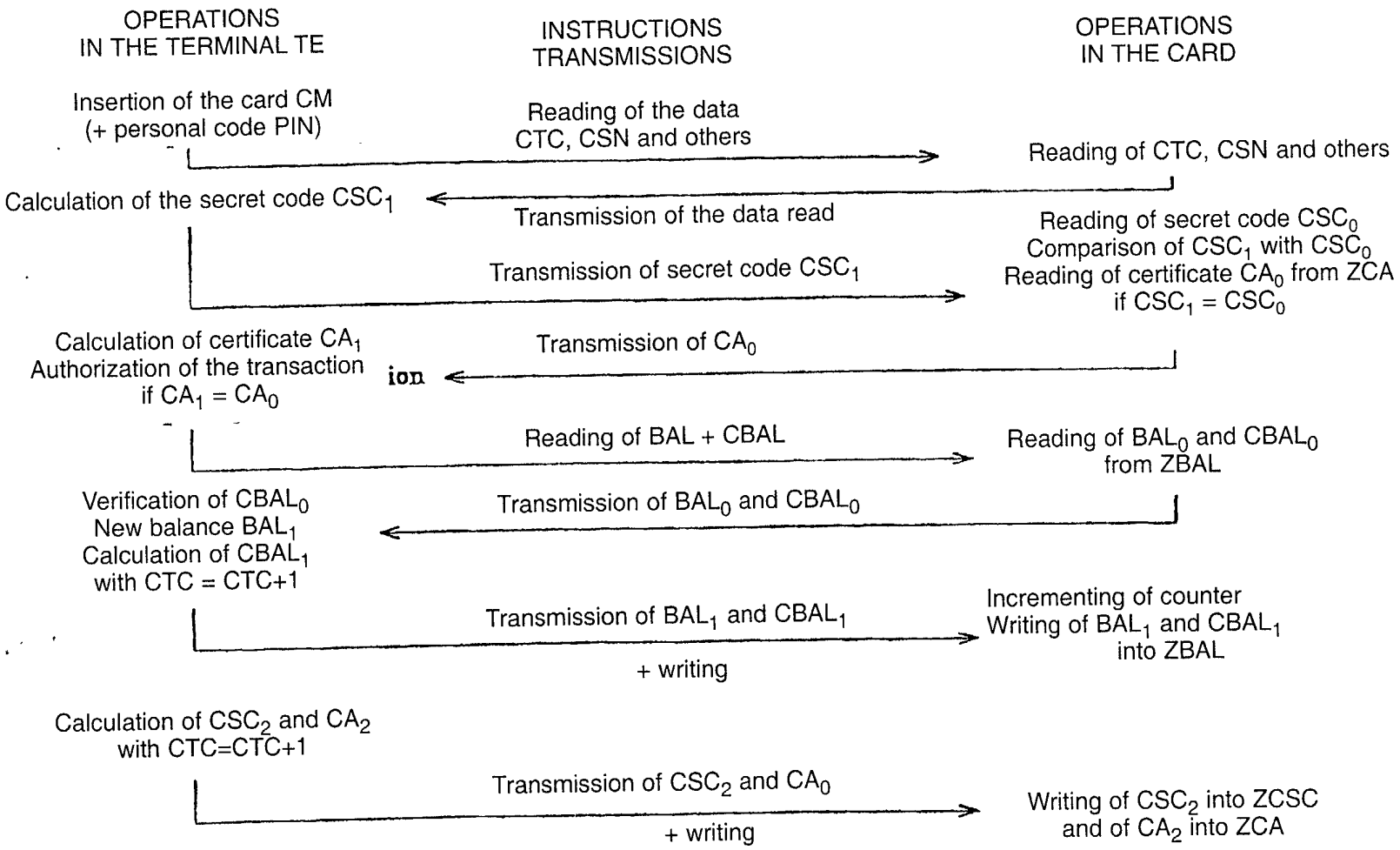

FIG.2

COMBINED DECLARATION AND POWER OF ATTORNEY FOR UTILITY PATENT APPLICATION	Attorney's Docket No. GEM 557

As a below-named inventor, I hereby declare that:
My residence, post office address and citizenship are as stated below next to my name;
I BELIEVE I AM THE ORIGINAL, FIRST AND SOLE INVENTOR (if only one name is listed below) OR AN ORIGINAL, FIRST AND JOINT INVENTOR (if more than one name is listed below) OF THE SUBJECT MATTER WHICH IS CLAIMED AND FOR WHICH A PATENT IS SOUGHT ON THE INVENTION ENTITLED:
AUTHENTICATING METHOD BETWEEN A SMART CARD AND A TERMINAL

the specification of which (check one) ☐ is attached hereto; ☐ was filed on as Application No. And was amended on ; (if applicable)

I HAVE REVIEWED AND UNDERSTAND THE CONTENTS OF THE ABOVE ~~IDENTIFIED SPECIFICATION~~, INCLUDING THE CLAIMS, AS AMENDED BY ANY AMENDMENT REFERRED TO ABOVE;

I ACKNOWLEDGE THE DUTY TO DISCLOSE TO THE OFFICE ALL INFORMATION KNOWN TO ME TO BE MATERIAL TO PATENTABILITY AS DEFINED IN TITLE 37, CODE OF FEDERAL REGULATIONS, Sec. 1.56 (as amended effective March 16, 1992);

I do not know and do not believe the said invention was ever known or used in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to said application; that said invention was not in public use or on sale in the United States of America more than one year prior to said application; that said invention has not been patented or made the subject of an inventor's certificate issued before the date of said application in any country foreign to the United States of America on any application filed by me or my legal representatives or assigns more than twelve months prior to said application;

I hereby claim foreign priority benefits under Title 35, United States Code Sec. 119 and/or Sec. 365 of any foreign application(s) for patent or inventor's certificate as indicated below and have also identified below any foreign application for patent or inventor's certificate on this invention having a filing date before that of the application(s) on which priority is claimed:

COUNTRY/INTERNATIONAL	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED
FR	98/14224	12/11/1998	YES
PCT	PCT/FR99/02692	4/11/1999	YES

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	R. Danny Huntington	27,903	Gerald F. Swiss	30,113
Robert S. Swecker	19,885	Eric H. Weisblatt	30,505	Michael J. Ure	33,089
Platon N. Mandros	22,124	James W. Peterson	26,057	Charles F. Wieland III	33,096
Benton S. Duffett, Jr.	22,030	Teresa Stanek Rea	30,427	Bruce T. Wieder	33,815
Norman H. Stepno	22,716	Robert E. Krebs	25,885	Todd R. Walters	34,040
Ronald L. Grudziecki	24,970	William C. Rowland	30,888	Ronni S. Jillions	31,979
Frederick G. Michaud, Jr.	26,003	T. Gene Dillahunty	25,423	Harold R. Brown III	36,341
Alan E. Kopecki	25,813	Patrick C. Keane	32,858	Allen R. Baum	36,086
Regis E. Slutter	26,999	Bruce J. Boggs, Jr.	32,344	Steven M. du Bois	35,023
Samuel C. Miller, III	27,360	William H. Benz	25,952	Brian P. O=Shaughnessy	32,747
Robert G. Mukai	28,531	Peter K. Skiff	31,917	Kenneth B. Leffler	36,075
George A. Hovanec, Jr.	28,223	Richard J. McGrath	29,195	Fred W. Hathaway	32,236
James A. LaBarre	28,632	Matthew L. Schneider	32,814		
E. Joseph Gess	28,510	Michael G. Savage	32,596		

21839

Address all correspondence to:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

21839

Address all telephone calls to: James LaBarre at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false state-ments and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF SOLE OR FIRST INVENTOR	SIGNATURE	DATE
Pascal COOREMAN		25/4/01
RESIDENCE		CITIZENSHIP
Les Jardins de l'Infante – 23, av Beau Pin – 13008 MARSEILLE / FRANCE FRX		FRANCE
POST OFFICE ADDRESS		
Les Jardins de l'Infante – 23, av Beau Pin – 13008 MARSEILLE / FRANCE		
FULL NAME OF SECOND JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE		CITIZENSHIP
POST OFFICE ADDRESS		

1-CO